

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

The residence located at 8405 Nicholson Road,
Caledonia, WI 53108. See Attachment A.

)
)
) Case No. 15-920M(NJ)
)
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

The residence located at 8405 Nicholson Road, Caledonia, WI 53108. See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

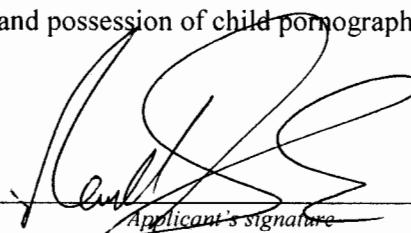
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of:

18 U.S.C. §§ 2252 and 2252A: illegal production, distribution, receipt and possession of child pornography.

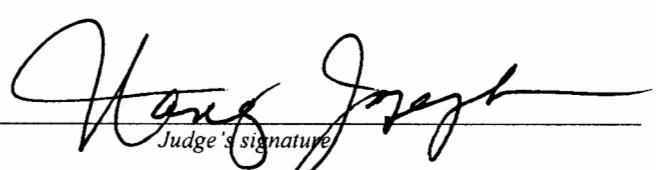
The application is based on these facts: See attached affidavit.



Special Agent Russell Dykema, DHS ICE HSI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: August 7, 2015



City and State: Milwaukee, Wisconsin

Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Russell A. Dykema, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), an investigative branch of the United States Department of Homeland Security. I am a federal law enforcement officer authorized by the Secretary of Homeland Security to request the issuance of criminal complaints and search warrants. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as a Special Agent for ICE/HSI, since June 2006. I am currently assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as storage devices, the Internet, and printed images).

2. This affidavit is submitted in support of an application for a search warrant for the residence located at 8405 Nicholson Road, Caledonia, Wisconsin 53108, more particularly

described in Attachment A (hereinafter "PREMISES,"), including electronic devices located therein, for evidence of violations of Title 18, United States Code, Section 2252A, entitled "Certain activities relating to material constituting or containing child pornography."

3. Based upon the information summarized in this affidavit, I have reason to believe that evidence of such violations may be present at the PREMISES.

4. The information supplied in this affidavit is based upon my investigation and information provided and investigation conducted by other law enforcement personnel in this matter to date that I consider reliable. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact related to or otherwise the product of this investigation.

DEFINITION OF TECHNICAL TERMS

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

6. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of numbers and/or characters often separated by periods (e.g., 121.56.97.178). Every device attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

7. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

TECHNICAL INFORMATION REGARDING DROPBOX

9. “Dropbox” refers to an online storage medium on the Internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the Internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted to only store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

10. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full name, physical address, telephone

numbers and other identifiers, alternate e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

11. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

12. Dropbox allows users to access and share their files on computers, phones, tablets, and the Dropbox website. Files or folders in a Dropbox account can be shared. The user can select a file or folder, then select "Share Link" from the Dropbox menu. Once this is done, the user can send the link to anyone over email, instant message, text message, blog posts, or anywhere they would like people to access the file copy. Persons who click the link will get a preview of the file or folder on the Dropbox website. They also have the option to download a copy of the file. If a video link is shared, the recipient will be able to watch up to 15 minutes of it on the preview page on the Dropbox website. For a longer video, the recipient will need to download the file or watch from the Dropbox mobile app to see all of it.

13. Dropbox links are secure. Dropbox creates a unique token used only in that link. According to Dropbox, "It is almost impossible to guess this token". When a link is created for a folder, everything in the folder and its subfolders will be accessible from the link. Moving items

out of the folder or removing the link to the folder will make the contents of the folder no longer available.

BACKGROUND OF THE INVESTIGATION

14. On January 15, 2015, HSI Tucson, Arizona, special agents executed a federal search warrant issued by the United States District Court, District of Arizona on the residence of Nathan NICKELL ("NICKELL"), located at 10193 E. Prospect Vista Way, Tucson, Arizona, for suspected violations of 18 U.S.C. § 2252, possession and distribution of child pornography.

15. Special agents seized several laptop computers, one Samsung Galaxy S4 cellular telephone, a Samsung Tablet, and external hard drives. One of the laptops that NICKELL identified as his was previewed and numerous anime¹ images depicting children having sexual intercourse with adults were found. A more extensive computer examination is ongoing.

16. HSI Tucson special agents conducted a forensic preview of NICKELL's Samsung Galaxy S4 cellular telephone. On January 26, 2015, special agents recovered over 200 thumbnail images in the cache for the Dropbox application that was installed on NICKELL's cellular telephone. Over 100 of these images are child pornography or child erotica images.

17. During a proffer session, NICKELL admitted that he regularly used various chat platforms to share links (Dropbox, Imgur², etc.) to child pornography material. NICKELL provided HSI special agents information indicating that he had stored numerous links to child pornography material in a Microsoft Word document stored on his laptop. HSI Tucson special agents extracted a Microsoft Word document file named, "red flag2.doc," that contained links to

¹ Anime is a style of animation originating in Japan that is characterized by stark colorful graphics depicting vibrant characters in action-filled plots often with fantastic or futuristic themes.

Dropbox accounts. One of the links was identified as:
“https://www.dropbox.com/sh/h3tdljnp78u8752/AACYYugCceXw7RSLBzDUBmgda/Video%20Jun%2016%2C%201%2052%2028%20AM.mp4.”

18. On April 3, 2015, a federal search warrant was signed in the United States District Court, for the District of Arizona, by United States Magistrate Judge Bernardo P. Velasco, for information from the Dropbox accounts that were associated with the Dropbox links recovered in the “redflag2.doc” file. The Dropbox accounts and associated Dropbox links are stored, owned, maintained, controlled, and/or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, California.

19. As a result of the search warrant, the Dropbox link:
“https://www.dropbox.com/sh/h3tdljnp78u8752/AACYYugCceXw7RSLBzDUBmgda/Video%20Jun%2016%2C%201%2052%2028%20AM.mp4” was identified as being created by the following account (referred to herein as “ACCOUNT #1”):

Name: Ashley
Email: sexyredhead@gmail.com
User: 308923525
Joined: 2014-06-16 04:33:10 (GMT)
Subscription Status: Unpaid

20. The content returned from Dropbox on ACCOUNT #1 includes 12 separate folders and hundreds of individual files contained within the folders. The majority of the files within the account are pornographic in nature. Some files are clearly adult pornography while others are clearly child pornography/child erotica. The files contain photographs, videos, screen shots of a cellular telephone screen, and other various electronic media. Also returned from

² Imgur is an online image hosting and comment-based social network community.

Dropbox was an excel spreadsheet showing a date/timestamp, user, file name, and file size for everything contained in ACCOUNT #1.

- a. Among the child pornography items located in ACCOUNT #1 is a folder titled, "Girl Time," and a video titled, "Video Mar 30, 10 35 28 PM.mp4." The video file is two minutes and forty four seconds in length. There is no audio associated with the file. The video portrays a prepubescent white female, with light brown or blonde hair, sitting naked on the floor of what appears to be a bedroom. The female has underdeveloped breasts and lacks pubic hair. The female appears to be engaging in a video chat and can be seen talking, typing, and adjusting the camera. The female can be seen spreading her legs and rubbing her vagina with her hand and fingers. The attached spreadsheet for the account indicates that this file was created on June 16, 2014 at 07:39:33 AM, by user 308923525.
- b. Also among the child pornography items located in ACCOUNT #1 is a folder titled, "Nudes (1)," and a video titled, "Video Apr 28, 4 30 56 PM.mp4." The video file is six minutes and thirty nine seconds in length. There is no audio associated with the file. The video portrays a prepubescent white female and a prepubescent white male, both with dark hair. Both individuals are fully clothed initially and partially clothed throughout different parts of the video. The female has underdeveloped breasts and lacks pubic hair. The male has underdeveloped genitals and lacks pubic hair. Both individuals appear to be engaging in a video chat and can be seen talking, typing, and adjusting the

camera. The female can be seen fondling the male's penis and performing oral sex on the male. The male can be seen sucking the breasts of the female and performing oral sex on the female. The male and female appear to attempt sexual intercourse. The female also bends over and pulls apart her vagina for the camera. The attached spreadsheet for this account indicates that this file was created on June 17, 2014 at 02:36:58 AM, by user 308923525.

21. In addition, Dropbox provided login timestamps and IP addresses for ACCOUNT #1:

Timestamp (GMT)	IP Address
2014-11-06 23:17:33	98.144.42.55
2014-11-06 23:19:21	98.144.42.55
2014-11-12 21:38:50	98.144.42.55
2014-11-13 20:41:57	98.144.42.55
2014-11-13 20:44:02	98.144.42.55
2014-11-20 03:04:18	98.144.42.55
2014-11-21 00:07:20	98.144.42.55
2014-12-03 20:55:03	98.144.42.55
2014-12-04 04:07:59	98.144.42.55
2014-12-05 01:40:07	98.144.42.55
2014-12-07 21:55:35	66.87.76.10
2014-12-09 00:46:59	98.144.42.55
2014-12-09 15:21:40	98.144.42.55
2014-12-10 17:07:13	98.144.42.55
2014-12-14 05:29:11	98.144.42.55
2014-12-17 17:04:05	98.144.42.55
2014-12-18 04:35:39	98.144.42.55
2014-12-20 19:48:02	66.87.77.168
2014-12-23 01:31:08	98.144.42.55
2015-01-01 01:20:41	98.144.42.55
2015-01-01 20:33:31	98.144.42.55
2015-01-02 23:38:38	66.87.76.228
2015-01-07 21:32:59	98.144.42.55
2015-01-10 02:14:31	98.144.42.55
2015-01-15 05:29:09	98.144.42.55

2015-01-15 05:29:55	98.144.42.55
2015-01-19 20:05:07	98.144.42.55
2015-01-21 02:25:26	98.144.42.55
2015-01-24 00:36:14	98.144.42.55
2015-01-25 22:02:42	98.144.42.55
2015-01-30 18:08:45	98.144.42.55
2015-02-05 05:23:18	98.144.42.55
2015-02-08 07:31:54	98.144.42.55
2015-02-15 23:38:05	98.144.42.55
2015-02-20 15:41:14	98.144.42.55
2015-02-22 05:27:05	98.144.42.55
2015-02-27 18:18:46	98.144.42.55
2015-03-02 16:06:49	66.87.76.246
2015-03-02 16:07:47	66.87.76.246

22. A search of Internet records shows that IP address 98.144.42.55 is registered to the ISP, Time Warner Cable. IP addresses 66.87.76.10 and 66.87.76.246 are registered to Sprint. An administrative summons was served on Time Warner Cable requesting the subscriber information for IP address 98.144.42.55 for the respective dates and times listed above. Time Warner Cable responded on May 26, 2015, with the following details about the subscriber:

Subscriber Name: Robert Proeber
Subscriber Address: 8405 Nicholson Rd, Caledonia, WI 53108-9619
Service Type: RR HSD
Active Date: 10/18/2007
Deactivate Date: Still Active
User Name or Features: RPROEBER3@wi.rr.com, projoe50@wi.rr.com, and mproeber1@wi.rr.com
Phone Number: (262) 327-XXXX

23. A driver's license query of Robert A. PROEBER (DOB: 06/13/1962) returned a valid Wisconsin driver's license (P616-7616-2213-01) issued on June 9, 2011 and valid until June 13, 2019 at 8405 Nicholson Road, Caledonia, Wisconsin 53108.

24. Database queries of vehicle registration indicate numerous vehicles registered to Robert A. PROEBER at 8405 Nicholson Road, Caledonia, Wisconsin 53108.

25. Database queries of other individuals residing at 8405 Nicholson Road, Caledonia, Wisconsin indicate at least two adult male children and one adult female residing at the residence.

26. The residence located at 8405 Nicholson Road, Caledonia, Wisconsin 53108, is within the Eastern District of Wisconsin.

27. On June 24, 2015, HSI Milwaukee agents traveled to 8405 Nicholson Road, Caledonia, Wisconsin and checked for unsecure wireless internet connections while parked adjacent to the residence. No unsecure wireless internet connections were found. There were three different wireless connections that appeared; however, they were all password protected.

28. On July 7, 2015, contact was made with the Caledonia Police Department (CPD) regarding PROEBER and the residence of 8405 Nicholson Road. CPD verified that 8405 Nicholson Road is the address of record for PROEBER. CPD found no derogatory information for PROEBER or the address 8405 Nicholson Road.

INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILD PORNOGRAPHY

29. Based on my training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals who create, possess, receive, distribute or access with intent to view child pornography have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement

officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. Many individuals who create and collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.
- b. Many individuals who create and collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found in email accounts that also contain child pornography, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.
- c. Many individuals who create and collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of

illicit materials. They almost always maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person.

- d. Many individuals who create and collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.
- e. Many individuals who create and collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.
- f. Many individuals who create and collect child pornography often collect, read, copy or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that

they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. This application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

31. Probable cause. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be

recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. Forensic evidence. This application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for

forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file

creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a

search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because it is possible that several people share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

36. Based on the facts as I have stated them in this affidavit, there is probable cause to believe that evidence of violations of Section 2252A of Title 18 of the United States Code is located at the PREMISES described further in "Attachment A." "Attachment B" to this affidavit is a list of items that would be the subjects of search and seizure at this location.

ATTACHMENT A

Property to be searched

The property to be searched is 8405 Nicholson Road, Caledonia, Wisconsin 53108, further described as a single story, single family residence, with tan brick, a brown roof, and attached garage. Affixed to the residence are the house numbers "8405" to the right of the southernmost entry door to the residence. The entry door has a brown screen door and a brown entry door. The location consists of the subject residence, and any included storage or garage space.

Photographs of this residence, taken on July 10, 2015, follow:



ATTACHMENT B

Property to be seized

1. All records relating to violations of Title 18, United States Code, Sections 2252A, including:
 - a. Records containing child pornography or pertaining to the distribution, receipt or possession of child pornography;
 - b. Records and information, notes, documents, records, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors.
 - c. Records evidencing occupancy or ownership of the premises described above, including but not limited to utility and telephone bills, mail envelopes, or addressed correspondence;
 - d. Cellular telephones, telephone and address books, and other notes and papers insofar as they memorialize, include, or confirm computer screen names, contact information, or images related to the sexual exploitation of children, in violation of Title 18, United States Code, Section 2252A;
 - e. Any and all cameras, film, videotapes or other photographic equipment that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of 18 U.S.C. § 2252A.
 - f. Credit cards, credit card information, bills and payment records pertaining to violations of 18 U.S.C. § 2252A.
 - g. Any and all records in any form or other items or materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence, including but not limited to sales receipts, invoices, bills for Internet access, and handwritten notes.
2. Computers and storage media used as a means to commit the violations described above, including receiving, possessing, and distributing child pornography in violation of 18 U.S.C. § 2252A.
3. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.
- j. records and things evidencing the use of the Internet Protocol address 98.144.42.55, 66.87.76.10 and 66.87.76.246 including:
 - i. routers, modems, and network equipment used to connect computers to the Internet;
 - ii. records of Internet Protocol addresses used;
- k. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet or P2P search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.